第 57 卷 第 8 期 2008 年 8 月
1000-3290/2008/57(08)/4689-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.57, No.8, August, 2008

具有双向认证功能的量子秘密共享方案*

孙 莹[1)2)†] 杜建忠[2)] 秦素娟[1)2)] 温巧燕[1)2)] 朱甫臣[3)]

1)(北京邮电大学网络与交换技术国家重点实验室,北京 100876)

2)(北京邮电大学理学院,北京 100876)

3)(现代通信国家重点实验室,成都 610041)

(2007 年 11 月 16 日收到;2008 年 3 月 6 日收到修改稿)

利用两粒子纠缠态作为经典信息的载体,结合 Hash 函数和量子本地操作提出了一种可以实现双向认证功能的量子秘密共享方案,并且分析了它的安全性. 这种方案的安全性基于秘密共享双方的认证密钥和传输过程中粒子排列次序的保密. 若不考虑认证和窃听检测所消耗的粒子,平均 1 个 Bell 态共享 2 bit 经典信息.

关键词:量子秘密共享,认证密钥,量子双向认证,两粒子量子纠缠

PACC:0367,0365

1. 引 言

假设 Alice 想将一个秘密计划交给远方的 Bob 和 Charlie 来共同完成,她对 Bob 或 Charlie 不是完全信任,但如果他们两人合作来完成这个任务,诚实的一方将会阻止不诚实的一方破坏该任务. 于是 Alice 将秘密计划分割成两部分,分别发给 Bob 和 Charlie,期望以此保证 Bob 和 Charlie 任何一人都不可能单独获得计划的内容,只有两人合作才能恢复出计划内容. 在与上述类似的各种场合中,秘密共享协议发挥了重要的作用.

秘密共享方案最早由 Shamir[1] 和 Blakley[2] 于 1979 年分别独立提出. 1999 年 Hillery, Bužek 和 Berthiaume[3] 提出了第一个量子秘密共享协议(HBB 协议). 在协议中,每个参与方持有 Greenberger-Horne-Zeilinger(GHZ)态的一个粒子,分别独立地随机选择 X 基和 Y 基之一进行测量,这与 1992 年由 Bennett 等[4] 提出的量子密钥分发协议类似. 自从 HBB 协议被提出以后,基于量子特性的秘密共享研究引起了人们的极大关注[5—22]. 与经典秘密共享不同的是,量子秘密共享不仅可以在通信者之间共享经典消息,也可以实现量子消息的共享. 我们的研究工作偏向于前者,最早的量子秘密共享协议(HBB 协议)就属于这一类,还有诸如基于两粒子纠缠态的秘密共享[5]、不需要纠缠的秘密共享[11]、多方与多方之间的秘密共享[14] 和利用单光子实现的秘密共享[15] 等众多方案都是用量子的方法来实现经典消息的共享.

在现实中存在这样一种情况,即会有非法的第三方冒充 Alice 发布假指令,企图指挥 Bob 和 Charlie 完成非法的任务. 但是在上面所提到的各类方案中,都事先就假设了 Alice 是合法的且 Bob 和 Charlie 至少有一个是可信的,即不考虑身份认证,而仅仅讨论消息的分割. 本文中,我们参考最近 Zhu 等在文献[23]中应用的一种利用粒子序列的重排列保证通信安全性的思想,提出了一种将认证结合进秘密共享的量子方案. 这种将 Einstein-Podolsky-Rosen(EPR)对的粒子对应关系打乱的思想最早在文献[24—26]中得到应用,Deng 等[16] 最早将该思想推广到量子秘密共享协议中. 本文所提出的方案基于 Hash 函数和量子本地操作完成认证功能,利用两粒子最大纠缠态在 Pauli 门作用下的变换将经典消息编码进量子态中,协议的安全性则由保密的 EPR 对的粒子对应关系来保证.

* 国家高技术研究发展计划(批准号:2006AA01Z419)、国家自然科学基金重大研究计划(批准号:90604023)、高等学校博士学科点专项科研基金(批准号:20040013007)、现代通信国家重点实验室基金(批准号:9140C1101010601)和北京市自然科学基金(批准号:4072020)资助的课题.

† E-mail:sunshiny2007@yahoo.cn

2. 具有双向认证能力的量子秘密共享方案

2.1. 编码机制与 PBS 工作原理

本文方案在认证过程中所需的准备工作与文献[27]提出的量子直接通信协议的认证部分类似. Bob 和 Charlie 分别与合法的命令发布者 Alice 共享一个代表自己身份的序列和一个 Hash 函数,身份序列和 Hash 函数对于任意第三方保密. Hash 函数的形式如下:

$$h:\{0,1\}^{*}\times\{0,1\}^{l}\rightarrow\{0,1\}^{N}, \tag{1}$$

其中上标星号表示输入的二进制序列可以是任意长度,l 表示计数器的二进制序列长度,N 表示输出的二进制序列长度. Hash 函数 $h_{\mathrm{Bob}}(S_{\mathrm{ID\text{-}Bob}},C_{\mathrm{Bob}})$ 和 $h_{\mathrm{Charlie}}(S_{\mathrm{ID\text{-}Charlie}},C_{\mathrm{Charlie}})$ 分别用来计算 Bob,Charlie 与 Alice 共享的认证密钥,$S_{\mathrm{ID\text{-}Bob(Charlie)}}$ 和 $C_{\mathrm{Bob(Charlie)}}$ 分别是 Bob(Charlie)的身份序列和 Hash 函数的计数器序列. 从(1)式可以看出,我们不必限制 $S_{\mathrm{ID\text{-}Bob}}$ 和 $S_{\mathrm{ID\text{-}Charlie}}$ 是等长的.

本文方案利用了 Pauli 矩阵的特殊性质将经典信息编码在 Bell 态上,以达到安全传输和共享的目的. 为了在实现 Alice 与 Bob,Charlie 之间的相互认证与秘密共享的同时不泄露认证密钥的信息,我们设计的方案要求 Bob 和 Charlie 在协议未进行到最后一步时不能泄露自己制备的单粒子的初态. 4 个 Pauli 矩阵分别为

$$U_0=I=|0\rangle\langle 0|+|1\rangle\langle 1|,$$
$$U_1=\sigma_x=|0\rangle\langle 1|+|1\rangle\langle 0|,$$
$$U_2=\mathrm{i}\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|,$$
$$U_3=\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|.$$

4 个 Bell 态分别表示如下:

$$|\phi^{+}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle), \tag{2}$$

$$|\phi^{-}\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle), \tag{3}$$

$$|\psi^{+}\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle), \tag{4}$$

$$|\psi^{-}\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle), \tag{5}$$

它们在 Pauli 矩阵的作用下相互转化的关系如表 1 所列.

表 1 Bell 态在 Pauli 矩阵作用下的相互转化

	$\|\phi^{+}\rangle$	$\|\phi^{-}\rangle$	$\|\psi^{+}\rangle$	$\|\psi^{-}\rangle$
$\|\phi^{+}\rangle$	$U_0(00)$	$U_3(11)$	$U_1(01)$	$U_2(10)$
$\|\phi^{-}\rangle$	$U_3(11)$	$U_0(00)$	$U_2(10)$	$U_1(01)$
$\|\psi^{+}\rangle$	$U_1(01)$	$U_2(10)$	$U_0(00)$	$U_3(11)$
$\|\psi^{-}\rangle$	$U_2(10)$	$U_1(01)$	$U_3(11)$	$U_0(00)$

Hadamard 矩阵 $H=\frac{1}{\sqrt{2}}(|0\rangle\langle 0|-|1\rangle\langle 1|+|0\rangle\langle 1|+|1\rangle\langle 0|)$ 可以实现 Z 基与 X 基之间的转换,并且 $H^2=I$. 在本文中,Hadamard 矩阵在身份认证和窃听检测的过程中起着关键作用.

同时,我们约定 U_0-U_3 分别对应以下经典信息编码(见表 1):$U_0\leftrightarrow 00$,$U_1\leftrightarrow 01$,$U_2\leftrightarrow 10$,$U_3\leftrightarrow 11$.

另外,为了窃取秘密分发者对单光子信号的操作,有一种常用的木马攻击——多粒子欺骗信号攻击. 这种攻击可以通过光子分数器(photon number splitter,简记为 PNS)来检测,但是由于 PNS 在目前的技术下并不可行,所以可以采用光子分束器(photon beam splitter,简记为 PBS)来实现对粒子欺骗信号的检测[28]. 为了能具有更良好的安全特性,可以使用 3 个或多个 PBS[29],具体的实现如图 1 所示.

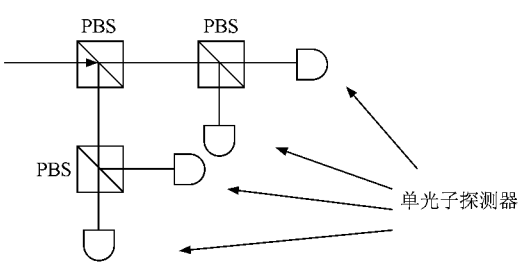

图 1 利用 PBS 实现多粒子欺骗信号的检测

秘密分发人 Alice 通过图 1 所示的装置将用于检测的样本中的每一个信号分裂后,用单光子探测器测量. 若分裂前的初始信号只包含一个光子,则只有一个探测器会探测到光子 若是多光子信号,则会有较大概率导致探测到光子的探测器数目多于 1. 这就是利用 PBS 实现多光子欺骗信号检测的原理.

2.2. 方案描述

本文所提出的具有双向认证功能的量子秘密共享方案可分为 7 个步骤.

第 1 步 Bob 和 Charlie 分别制备 N 个随机处

于 $\{|0\rangle,|1\rangle\}$ 之一的单光子，形成的两个序列分别记为 S_B 和 S_C. Bob 根据自己的认证密钥 $h_{Bob}(S_{ID\text{-}Bob},C_{bob})$ 对 S_B 中每一个光子进行如下操作：若 $h_{Bob}(S_{ID\text{-}Bob},C_{Bob})$ 的第 i 个值是 0，则 Bob 对序列 S_B 中的第 i 个光子做一次 I 操作；若 $h_{Bob}(S_{ID\text{-}Bob},C_{Bob})$ 的第 i 个值是 1，则 Bob 对序列 S_B 中的第 i 个光子做一次 H 操作. 同时，Charlie 也根据自己的认证密钥 $h_{Charlie}(S_{ID\text{-}Charlie},C_{Charlie})$ 对 S_C 中每一个光子进行如上的操作. 完成上述操作后，Bob 和 Charlie 将 S_B 和 S_C 发给 Alice.

第 2 步　Alice 收到 S_B 和 S_C 后，根据自己拥有的认证密钥 $h_{Bob}(S_{ID\text{-}Bob},C_{Bob})$ 和 $h_{Charlie}(S_{ID\text{-}Charlie},C_{Charlie})$ 对 S_B 和 S_C 中的光子分别进行与第 1 步相同的操作. 为了抵御多粒子欺骗信号攻击，接下来 Alice 从 S_B 和 S_C 中选出足够多的光子作为样本粒子（假设两个序列中的样本数均为 $N-n$），让它们依次通过图 1 所示的设备（PBS 的分束比为 50∶50），光子探测器的测量基从 Z 基和 X 基中随机选取. 若检测到多光子的概率高于事先确定的门限值，Alice 宣布该次通信作废，通知 Bob 和 Charlie 从第 1 步重新开始. 否则，Alice 开始对 Bob 和 Charlie 进行认证：她公布样本粒子的位置和所有测量结果，由 Bob 和 Charlie 对比自己制备时的初态宣布哪些位置的测量结果不相符，若错误率高于事先确定的门限值，则 Alice 宣布取消该次通信，认为 Bob 或（和）Charlie 非法，或者 Bob 或（和）Charlie 与 Alice 之间的量子信道存在恶意扰乱. 此时，由 Alice 决定是否进行新一轮的秘密共享. 否则，继续进行下一步.

第 3 步　Alice 从两个序列中分别取出第 i 个光子（$i=1,2,\cdots,n$），对它们进行 Bell 基测量. 然后根据测量结果制备一个相同的纠缠态，记第 i 个纠缠态为 $|\Psi_i\rangle$，其中对应属于 Bob 的粒子称为粒子 B，另一个粒子称为粒子 C.

第 4 步　全部测量完毕以后，Alice 从自己拥有的这 n 个纠缠态中随机选出一个足够大的子集，用于窃听检测，记这个集合为 C_A. 剩余的纠缠态作为 Alice 要共享秘密的载体，记为 M_A. Alice 将自己要共享的秘密编码为幺正操作：$00\leftrightarrow U_0$，$01\leftrightarrow U_1$，$10\leftrightarrow U_2$，$11\leftrightarrow U_3$，依次作用在集合 M_A 中每一纠缠态的粒子 B 上. 对于集合 C_A 中的纠缠粒子对，Alice 随机选取 U_0，U_2 作用在纠缠态的粒子 B 上.

第 5 步　完成上述操作后，Alice 从 n 个处于纠缠态的粒子对里面将粒子 B 取出，形成一个新的序列，打乱次序后记为序列 S'_B，发给 Bob. 将粒子 C 也取出，形成新的序列，打乱次序后记为序列 S'_C，发给 Charlie. Alice 对 S'_B 和 S'_C 中的粒子次序保密.

第 6 步　Bob 和 Charlie 收到 S'_B 和 S'_C 后通知 Alice，Alice 公布各序列中 C_A 的位置（注意，这里并不公布 C_A 的秘密顺序，即 Bob 和 Charlie 不知道彼此检测粒子的秘密顺序），让 Bob 和 Charlie 分别测量并公布测量结果，Bob 和 Charlie 谁先公布结果可以由 Alice 随机决定. Alice 根据 C_A 的秘密顺序和他们的测量结果来决定错误率，从而完成对该次传输过程的窃听检测. 若错误率大于事先约定的门限值，则取消该次通信. 否则，继续进行下一步.

第 7 步　Alice 分别告知 Bob 和 Charlie 关于 S'_B 和 S'_C 中粒子的秘密顺序，并且按顺序宣布自己对未编码纠缠态的 Bell 基测量结果. Bob 和 Charlie 合作时，首先对 Alice 进行反向认证：两人分别出示在第 1 步制备的单粒子的初态，对照 Alice 宣布的两粒子纠缠对的初态（表 2），若错误率高于事先约定的门限值，则认为 Alice 是非法的，可以直接选择中止重建秘密. 否则，认为 Alice 是合法的.

表 2　单光子的初态与纠缠光子对的初态对应关系

	$\|0\rangle_B$	$\|1\rangle_B$
$\|0\rangle_C$	$\|\phi^+\rangle_{BC}$，$\|\phi^-\rangle_{BC}$	$\|\psi^+\rangle_{BC}$，$\|\psi^-\rangle_{BC}$
$\|1\rangle_C$	$\|\psi^+\rangle_{BC}$，$\|\psi^-\rangle_{BC}$	$\|\phi^+\rangle_{BC}$，$\|\phi^-\rangle_{BC}$

注：下标 B 和 C 分别代表粒子 B 和粒子 C.

认证结束后，开始重建秘密. Bob 和 Charlie 拿出各自拥有的粒子排列顺序正确的序列，对每一对应位置的粒子 B 和粒子 C 进行 Bell 基测量，根据 Alice 宣布的纠缠对初态，与表 1 对照后，即可重建 Alice 的秘密.

3. 安全性分析

3.1. 针对窃听者 Eve 和不诚实的参与方 D-Bob 的讨论

假设存在窃听者 Eve，她的目的就是分析 Alice 的操作或者获得 Bob 和 Charlie 的认证密钥或身份序列，并不被检测到. 下面，我们通过分析证明本文所提出的方案是安全的. 由于 Bob 和 Charlie 合法地

拥有部分秘密信息,并且在认证和窃听检测过程中有条件地通过公布虚假信息来掩盖自己的攻击痕迹,所以他们比外部窃听者 Eve 具有更大的攻击优势[30—32]. 可以这样认为,如果能够通过窃听检测发现参与方的窃听,那 Eve 的窃听行为同样会被检测到. 所以,我们针对 Bob 或 Charlie 是不诚实的情况进行下面的讨论.

假设参与方 Bob 不诚实(记不诚实的 Bob 为 D-Bob),他企图采取"截获-重发"和"纠缠-测量"攻击(这是两种常用的攻击手段)来获得 Charlie 的合法粒子所携带的信息,并成功逃避窃听检测. 假设 D-Bob 制备了 N 个$|\phi^+\rangle$,将每一个$|\phi^+\rangle$中的一个粒子冒充 Charlie 的粒子发送给 Alice,并截获 Charlie 的合法粒子,或者在 Alice 完成编码后发回给 Charlie 时截获粒子,而将$|\phi^+\rangle$中的一个粒子冒充合法粒子发给 Charlie.

首先,D-Bob 不可能通过这种方法不被检测地获得关于 Charlie 的认证密钥信息. 即使他截获了 Charlie 发给 Alice 的粒子,由于序列 S_C 中每一个粒子的初态都随机处于 $\{|0\rangle,|1\rangle\}$之一,密度矩阵为

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}I,$$

即每一个粒子都处于最大混合态. 所以无论是单纯地测量所截获的粒子,还是利用第 2 步中认证检测过程所公布的信息,D-Bob 都不能获得任何有效信息.

其次,由于 D-Bob 不知道 C_A 在 S'_C 中秘密顺序,导致了 D-Bob 对集合 C_A 中的任意一个纠缠态的两个光子在 S'_B 和 S'_C 两个序列中的位置对应关系都一无所知,于是在第 6 步的认证和检测过程中,D-Bob 只能随机猜测自己公布的每一个测量结果与 Charlie 所公布结果的关系,所以有 1/2 的概率猜错. 实际上,由于在步骤 6 的认证和检测过程只有 Alice 掌握了 C_A 分别在 S'_B 和 S'_C 中的秘密顺序,所以无论 D-Bob 何种攻击都会在这一步引入 1/2 的错误率.

另外,第 2 步和第 6 步的窃听检测是基于对错误率的统计分析,即使考虑实际的量子信道中存在噪声和损耗的因素,但是由于在非理想的条件下,由窃听或认证错误造成较高的错误率仍然会使三方取消该次通信,所以该方案在非理想情况下仍然是安全的.

3.2. 关于对 Alice 认证的安全性讨论

记企图冒充 Alice 的非法第三方为 D-Alice.

首先,该方案先由 Bob 和 Charlie 制备单光子发给 Alice,然后再由 Alice 作认证操作和 Bell 基测量. 所以,D-Alice 不可能通过纠缠交换的方法获取 Bob 和 Charlie 的合法认证密钥.

其次,D-Alice 不可能通过 Bob 和 Charlie 发来的粒子序列分析出他们的认证密钥. 这与上述 D-Bob 不能通过分析 Charlie 的粒子获得其认证密钥的原因是一样的.

再次,在 Bob 和 Charlie 合作对 Alice 进行认证时,因为 Bob 和 Charlie 制备的每个单光子随机地处于$|0\rangle$态或$|1\rangle$态,所以 Alice 对一对光子进行 Bell 基测量后,根据 Bob 和 Charlie 所制备光子的初始态是否相同,纠缠态有以下两种可能:若初态相同,则是$|\phi^+\rangle_{BC}$或$|\phi^-\rangle_{BC}$;若初态相反,则是$|\psi^+\rangle_{BC}$或$|\psi^-\rangle_{BC}$(表 2). 因此,根据已知信息并对照表 2 就可以发现 Alice 是否真正拥有 Bob 和 Charlie 的认证密钥,即可判断 Alice 是否合法.

例如,假设 Bob 和 Charlie 在序列 S_B 和 S_C 第 i 位置上所制备光子的初始态分别为$|0\rangle$和$|1\rangle$,Bell 基测量的结果应该是$|\psi^+\rangle_{BC}$或$|\psi^-\rangle_{BC}$. 但由于 D-Alice 不知道 Bob 和 Charlie 的认证密钥,所以在第 2 步做反向认证的操作时,D-Alice 猜错的概率 P_e 为 1/2. 假设 Bob 在该位置的认证密钥是 0,且 D-Alice 猜错了 Bob 的认证密钥($P_e = 1/2$),则她在收到 Bob 的序列后,会对这个位置的光子做一次 H 操作,这时该光子态将由$|0\rangle$变为$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. 于是,纠缠后的光子对可能处于$\{|\phi^+\rangle_{BC},|\phi^-\rangle_{BC},|\psi^+\rangle_{BC},|\psi^-\rangle_{BC}\}$四态之一,测量后的纠缠态就有 1/2 的可能性是属于集合$\{|\phi^+\rangle_{BC},|\phi^-\rangle_{BC}\}$. 从表 3 可以看出,假如 D-Alice 最后宣布 k 个纠缠对的初态,则在理想状态下被检测到的概率为 $1-\left(\frac{3}{4}\right)^k$.

在非理想量子信道条件下,根据信道噪声和损耗的各项参数,事先确定一个门限值,只要 Bob 和 Charlie 发现认证 Alice 的错误率高于该门限值,即可认为 Alice 是假冒的,从而取消该次任务.

表 3　认证过程中 D-Alice 对每个纠缠对引入的错误率

	Bob	Charlie	概率	Bell 测量出错概率	最终出错概率
D-Alice	×	√	1/4	1/2	1/4
	√	×	1/4	1/2	
	×	×	1/4	0	0
	√	√	1/4	0	

注：表中符号 × 表示 D-Alice 猜错 Bob/Charlie 的认证密钥，符号 √ 表示 D-Alice 猜对 Bob/Charlie 的认证密钥.

3.3. 其　他

最近，Cai[33] 提出一种基于光子探测器局限性的不可见光子攻击方案. 在该方案中，窃听者截获合法通信过程中的光子，将与合法通信所使用光子的波长相差较大的光子插入到粒子序列中，重新发送给接收方. 由于单光子探测器的局限性，无法检测到与合法光子波长相差较大的光子信号，所以也就无法防御这种不可见光子的攻击. 针对这种攻击，在第 2 步的检测和第 3 步的测量过程中，Alice 处理每一个光子信号之前都需要让该信号通过一个滤波器[28,34]. 该滤波器能够滤除与合法通信所使用光子信号的波长相差较大的光波，只允许合法波长(或者波长很接近合法波长)的光信号通过.

文献[34]指出，对于二次传输的光子序列，在合法信号中延迟一段时间(该延迟时间小于光学设备用于探测合法信号的时间窗口)插入欺骗信号，同样是一种有效的攻击策略，该攻击称为延迟光子木马攻击. 在本文方案中第 2 步检测多粒子欺骗信号攻击的过程中，所使用的检测装置(图 1)可以有效地防御这种攻击.

4. 结　　论

本文利用了将所传输的粒子次序重排列来保证秘密共享协议的安全性. 与文献[16]不同的是，本文提出的方案是由 Bob 和 Charlie 分别制备单粒子，然后传给 Alice，由 Alice 先对 Bob 和 Charlie 进行认证，然后再将要共享的秘密编码在已经实现纠缠的量子态上打乱顺序后分别发送给 Bob 和 Charlie，最后由 Bob 和 Charlie 完成对 Alice 的认证，并合作进行测量恢复出秘密. 该方案实现了在秘密共享的过程中完成双方的双向认证，不仅不需要事先做出‘秘密共享参与方 Bob 和 Charlie 至少有一个是可信的’的假设，而且能有效地防止攻击者企图假冒 Alice 发布伪造的命令.

除了具有较良好的安全特性，本文的方案还具有很高的量子比特效率. 根据量子比特效率的定义 $\eta_q = \frac{q_u}{q_t}$(q_u 表示最终有效的量子比特数，q_t 表示通过量子信道传输的总比特数)，除了窃听检测和身份认证所消耗的量子比特外，该方案中传输的所有量子比特最后都用于有效地传输秘密消息，所以在理论上 $\eta_q \approx 100\%$.

[1] Shamir A 1979 *Commun. ACM* **22** 612
[2] Blakley G R 1979 *Nat. Comput. Conf.* **48** 313
[3] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[4] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 3121
[5] Karlsson A, Koashi M, Imoto N 1999 *Phys. Rev.* A **59** 162
[6] Cleve R, Gottesman K, Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[7] Gottesman D 2000 *Phys. Rev.* A **61** 042311
[8] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308
[9] Tittel W, Zbinden H, Gisin N 2001 *Phys. Rev.* A **63** 042301
[10] Karimipour V, Bahraminasab A 2002 *Phys. Rev.* A **65** 042320
[11] Guo G P, Guo G C 2003 *Phys. Lett.* A **310** 247
[12] Bagherinezhad S, Karimipour V 2003 *Phys. Rev.* A **67** 044302
[13] Hsu L Y 2003 *Phys. Rev.* A **68** 022306
[14] Yan F L, Gao T 2005 *Phys. Rev.* A **72** 012304
[15] Deng F G, Zhou H Y, Long G L 2005 *Phys. Lett.* A **337** 329
[16] Deng F G, Long G L, Zhou H Y 2005 *Phys. Lett.* A **340** 43
[17] Yang Y G, Wen Q Y, Zhu F C 2006 *Acta Phys. Sin.* **55** 3255 (in Chinese) [杨宇光、温巧燕、朱甫臣 2006 物理学报 **55** 3255]
[18] Takesue H, Inoue K 2006 *Phys. Rev.* A **74** 012315
[19] Chen P, Deng F G, Long G L 2006 *Chin. Phys.* **15** 2228
[20] Zhang Y Q, Jin X R, Zhang S 2006 *Chin. Phys.* **15** 2252
[21] Zhou P, Li X H, Deng F G, Zhou H Y 2007 *Chin. Phys.* **16** 2867
[22] Man Z X, Xia Y J, An N B 2007 *Eur. Phys. J.* D **42** 333
[23] Zhu A D, Xia Y, Fan Q B, Zhang S 2006 *Phys. Rev.* A **73** 022338
[24] Deng F G, Long G L 2003 *Phys. Rev.* A **68** 042315
[25] Long G L, Liu X S 2002 *Phys. Rev.* A **65** 032302
[26] Deng F G, Long G L, Liu X S 2003 *Phys. Rev.* A **68** 042317
[27] Lee H, Lim J, Yang H J 2006 *Phys. Rev.* A **73** 042305
[28] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[29] Deng F G, Li X H, Zhou H Y, Zhang Z J 2005 *Phys. Rev.* A **72** 044302
[30] Qin S J, Gao F, Wen Q Y, Zhu F C 2006 *Phys. Lett.* A **357** 101
[31] Gao F, Qin S J, Wen Q Y, Zhu F C 2007 *Quantum Inf. Comput.* **7** 329
[32] Gao F, Wen Q Y, Zhu F C 2007 *Phys. Lett.* A **360** 748
[33] Cai Q Y 2006 *Phys. Lett.* A **351** 23
[34] Li X H, Deng F G, Zhou H Y 2006 *Phys. Rev.* A **74** 054302

Quantum secret sharing with bidirectional authentication*

Sun Ying[1)2)†] Du Jian-Zhong[2)] Qin Su-Juan[1)2)] Wen Qiao-Yan[1)2)] Zhu Fu-Chen[3)]

1) (*State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

2) (*School of Science*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

3) (*State Key Laboratory for Modern Communications*, *Chengdu* 610041, *China*)

(Received 16 November 2007; revised manuscript received 6 March 2008)

Abstract

A quantum secret sharing scheme with two-way authentication was proposed and discussed. Based on two-particle quantum entanglement, the scheme is implemented using the Hash function and the quantum local operations. The authentication keys and the secret order of transmitted particles ensure the security of the scheme. One Bell state can be used to share two classical bits on average if the particles for authentication and eavesdropping detection are not concernred.

Keywords: quantum secret sharing, authentication key, quantum bidirectional authentication, two-particle quantum entanglement

PACC: 0367, 0365

* Project supported by the National High Technology Development Program of China (Grant No. 2006AA01Z419), the Major Research Plan of the National Natural Science Foundation of China (Grant No. 90604023), the Doctoral Program Foundation of Institution of Higher Education of China (Grant No. 20040013007), the Foundation of State Key Laboratory for Modern Communications, China (Grant No. 9140C1101010601) and the Natural Science Foundation of Beijing, China (Grant No. 4072020).

† E-mail: sunshiny2007@yahoo.cn